NASA Procedural Requirements

NPR 1620.3
Effective Date: August 12, 2004
Expiration Date: August 12, 2009

COMPLIANCE IS MANDATORY

Physical Security Requirements for NASA Facilities and Property

Responsible Office: Office of Security & Program Protection

Table of Contents

CHAPTER 4: Minimum Physical Security Requirements for Other Categories of NASA Property not Subject to Physical Security Vulnerability Risk Assessments

CHAPTER 5: Keys, Locks, Locking Devices (Including Hasps and Chains), and Protective Seals

CHAPTER 6: Protective Barriers

Preface

P.1 Purpose.

This NPR outlines physical security requirements and responsibilities for safeguarding NASA assets. Its objectives are to:

a. Establish standardized physical security requirements for specific categories of NASA assets.

b. Base physical security requirements on an established physical security vulnerability risk assessment process, outlined in NPR 1620.2, "NASA Physical Security Vulnerability Risk Assessments," that allows Center management the flexibility to 1). Prioritize assets based on their risk level and criticality to the overall mission and, 2). Tailor risk level 2 and 3 security requirements to meet local needs provided that risk level 1 or other more appropriate compensatory physical security enhancements have been implemented. Risk level definitions are as follows:

1). Risk Level I - Assignment of this risk level designation indicates that the asset has been appropriately assessed and, due to its criticality and attractiveness, determined to be at the lowest level of risk for threat by criminals, terrorists, protestors, or other aggressors.

2). Risk Level II - Assignment of this risk level designation indicates that the asset has been appropriately assessed and, due to its criticality and attractiveness, determined to be at the mid-level of risk for threat by criminals, terrorists, protestors, or other aggressors.

(3). Risk Level III - Assignment of this risk level designation indicates that the asset has been appropriately assessed and, due to its criticality and attractiveness, determined to be at the highest level of risk for threat by criminals, terrorists, protestors, or other aggressors.

c. Reduce loss, theft, misuse, and damage of NASA assets cost effectively.

P.2 Applicability

This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities, to the Jet Propulsion Laboratory (JPL), and NASA contractors to the extent specified in their contracts. Address comments regarding this NPR to the Director, Security Management Office (DSMO), Office of Security Management and Safeguards, NASA Headquarters, Washington, DC, 20546. Refer questions concerning the application of these requirements to specific NASA Centers to the appropriate NASA Center Security Office.

P.3 Authority

a. 42 U.S.C., Section 2473(c)(1), National Space Program.

b. NASA Policy Directive 1600.2C, NASA Security Policy.

P.4 References

a. 14 CFR, Section 1203, National Aeronautics and Space Administration.

b. NASA Procedural Requirements (NPR) 1600.1, NASA Security Program Procedural Requirements.

c. NPR 1600.2, Physical Security Vulnerability Risk Assessments

d. NPR 4200.1, NASA Equipment Manual

e. NPR 4310.1, Identification and Disposition of NASA Artifacts

f. Presidential Decision Directive (PDD) 62, Combating Terrorism

g. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.

h. Government Accounting Office (GAO) - 02-95, Vulnerability Assessment of Federal Facilities, October 1995.

i. GAO - 03-08, Building Security - Security Responsibilities for Federally Owned and Leased Facilities, October 2002.

j. PDD 67, Enduring Constitutional Government and Continuity of Government Operations.

k. PDD 62, Countering Terrorism.

l. NPR 8820.2, NASA Construction of Facilities Procedural Requirements.

P.5 Cancellation

None

/S/
David A. Saleeba
Assistant Administrator
Office of Security and Program Protection

CHAPTER 1: General

1.1 Responsibilities

1.1.1. The Assistant Administrator, Office of Security Management and Safeguards (AA/OSMS), Code X, shall:

a. Provide overall policy direction and procedural requirements for the physical security of NASA assets (critical and non-critical).

b. Coordinate with Institutional Program Offices (IPO) and Center Directors, as necessary, to ensure appropriate application of established physical security policy, procedures, and requirements pertaining to the protection of NASA assets.

1.1.2. Center Directors shall:

a. Ensure Center security personnel conduct the appropriate physical security vulnerability risk assessment for all assets under their control in a timely manner.

b. Ensure senior management officials at their respective Center implement physical security measures commensurate with the requirements established in this NPR.

1.1.3. Center Chiefs of Security shall:

a. To the extent possible, ensure a physical security vulnerability risk assessment is conducted for all assets under their control in a timely manner. At a minimum, all Minimum Essential Infrastructure (MEI) assets, as defined in NPR 1600.1, NASA Security Program Procedural Requirements, shall be subject to the appropriate security vulnerability risk assessment immediately upon designation as critical infrastructure and/or key resource.

b. Ensure the physical security measures identified in this NPR are implemented as soon as practical, after funding is identified through the budgetary process.

c. As appropriate and required, notify the NASA Office of Inspector General of all crimes at NASA owned and/or leased facilities, to include theft or misuse of, or damage to, Government property.

1.1.4. Organizational Heads shall control and safeguard all property within their activity. They shall:

a. Promptly report to the Center law enforcement/security organization, and assist in any investigative activity and resolve incidents involving loss, theft, misuse, or damage of NASA resources.

b. Establish end-of-day security checks using Standard Form (SF) 701 (Activity Security Checklist) when storing classified or sensitive but unclassified information and material.

c. Implement security measures commensurate with the results of the physical security vulnerability

risk assessment conducted by Center security personnel.

1.1.5. Organizations involved in logistic and supply operations shall protect supplies and equipment as indicated in this NPR.

1.1.6. Facility Security Managers shall ensure periodic physical security inspections are conducted per local Center security policies and procedures.

1.1.7. Organizations assigned custody of controlled medical substances shall implement measures to safeguard them as required by this NPR. These responsibilities include:

a. Ensuring physical security responsibilities are fixed in the receipt, storage, issue, transportation, use, disposal, turn-in, and accounting for all controlled medical substances and sensitive items.

b. Providing specific security instructions to individuals who are in the possession and control of, or who are responsible for, controlled medical substances and sensitive items.

c. Ensuring the careful selection of personnel, including volunteer workers, who are assigned duties that require access to controlled medical substances and sensitive items storage areas or who have custodianship or possession of keys and combinations to locks securing these areas.

d. Taking action to deny access to controlled substances by individuals undergoing investigation, treatment, rehabilitation, or administrative action as a result of actual or suspected drug abuse or as a result of suspected illegal activity involving controlled drugs (for example, theft, wrongfully prescribing, and inventory manipulation.)

e. Establishing appropriate escort procedures and designating escort personnel, by name or duty position, to escort unauthorized people into storage areas.

f. Ensuring a Facility Security Coordinator (FSC) is appointed, in writing, by the medical facility manager to assure that appropriate protection is provided for all controlled medical substances and sensitive items.

1.2 Security Measures And Requirements

a. Physical security measures more stringent than those contained in this NPR may be implemented by a Center official based on the criticality or "value" of the asset under consideration, analysis of local threat, identified vulnerabilities, and available security resources. These measures shall be incorporated into the Center's physical security plan as an annex or as a mission specific security plan.

b. Provisions for security program funding shall be included in normal budget deliberations. Tenant activities shall coordinate their security program status, and when appropriate, security requirements to the host installation, so support may be provided at reimbursable cost, as appropriate.

c. Provision of security measures beyond those required by this NPR and other NASA procedural requirements shall be determined on a case-by-case basis by the Center Chief of Security (CCS).

1.3 Physical Security Measures for Stand-Alone Facilities or Facilities Located in Foreign Countries

1.3.1. Stand-alone or single facilities not located on U.S. Government installations or situated in foreign countries shall be secured as indicated below:

(1) Use of NASA photo-identification to facilitate entry of authorized personnel.

(2) Use of a centrally managed electronic access control system and integrated video surveillance to facilitate access for authorized personnel and provide real time feedback on suspicious activity.

(3) Installation of firearms, explosives, and nuclear/biological/chemical detection capability at visitor entry points.

(4) Centralized mail/shipping and receiving activity equipped with package screening capability.

(5) Entry points manned by qualified security personnel.

(6) Visitor reception and processing office.

1.3.2. When part of a multi-facility complex that is external to a NASA Center, including in an overseas environment, the measures outlined in paragraph 1.3.1, above, Risk Level II procedures outlined in section 3.19, and terrorism counter-measures outlined in section 3.20, shall be implemented to the extent appropriate, as determined by a physical security vulnerability risk assessment, postulated threat, and any international agreements.

1.4 Risk Management and Risk Acceptance Process

1.4.1. Management and security may disagree on the level of security required for a particular asset. When management disagrees on the level of security required, they may opt to acknowledge and accept the risk of implementing less stringent security measures than those required through the risk assessment process established in NPR 1620.2, NASA Physical Security Vulnerability Risk Assessment, provided the asset is not a national security asset. In the case of a national security asset, only the Assistant Administrator for Security Management and Safeguards may accept the risk.

1.4.2. Every effort will be made to resolve the differences at the Center level. Management will:

a. Document their position regarding the required security measures, and outline their recommended alternative approach.

b. Include any pertinent information, including an acknowledgement of risk.

c. Submit to the Center Chief of Security, who will review and concur/non-concur, as appropriate.

e. If concurrence is given, no further action is necessary. A copy of all documentation will be maintained at the Center security office.

f. If the review results in a nonconcurrence, the security office must provide appropriate rationale and justification for the nonconcurrence.

g. If an agreement between the security office and management cannot be reached, the issue must be presented to the appropriate senior management for resolution.

3.5.2. When senior management cannot resolve the impasse, or when the issue involves a national security asset, a request for waiver or exception of requirements must be processed in accordance with section 1.3, Chapter 1, NPR 1600.1, NASA Security Program Procedural Requirements.

1.5 Terms, Abbreviations, and Acronyms

Terms, abbreviations, and acronyms used in this NPR are explained in Chapter 10 of the parent

document, NPR 1600.1, NASA Security Program Procedural Requirements.

CHAPTER 2: Physical Security Vulnerability Risk Assessments

2.1 General

2.1.1. To provide the most practical physical protection for NASA assets, NASA managers must identify their mission essential critical assets and analyze the risks to those assets from damage and/or destruction from espionage, sabotage, terrorism, misuse, and theft.

2.1.2. Assessment of these risks shall assist in determining the type and minimum level of physical protection needed to safeguard the identified MEI resources adequately and economically. The objectives of a physical security vulnerability risk analyses are the following:

a. Provide NASA managers a tool with which to design a security program based on local needs.

b. Allow the flexibility to adapt risk level 2 and 3 physical security measures, as appropriate, to meet local risk conditions, provided risk level 1 or comparable security measures are in place and effective. In asset categories where physical security requirements have only been set at the higher risk levels, Center Security Offices shall develop minimum physical security requirements that provide for the appropriate level of security commensurate with the postulated threat.

c. Obtain the maximum return possible from invested resources.

d. Serve as a basis for an asset-specific threat analysis.

2.2 Use Of Physical Security Vulnerability Risk Assessments

2.2.1. The background and explanation of step-by-step procedures for conducting a physical security vulnerability risk assessment for categories of NASA assets and determining minimum security requirements are contained in NPR 1620.2, Physical Security Vulnerability Risk Assessments.

2.2.2. A physical security vulnerability risk assessment shall initially be conducted for assets that NASA Center Directors, and/or Enterprise/IPO managers have determined are part of the NASA critical infrastructure established under Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization, and Protection" as outlined in Chapter 8, paragraph 8.4 and Appendix H, NPR 1600.1, NASA Security Program Procedural Requirements.

2.2.3. The physical security vulnerability risk assessment can also be used to assist Centers in meeting the intent of PDD 67, "Enduring Constitutional Government and Continuity of Government Operations" and PDD 62, "Countering Terrorism."

2.2.4. Subsequent physical security vulnerability risk assessments shall be conducted on all NASA asset categories in a timely manner in accordance with the following:

a. When an activity is activated.

b. When an organization permanently relocates to a new site or facility.

c. When no formal record exists of a prior risk assessment.

d. Every 3 years or more frequently at the discretion of the Center Director.

e. During the planning stages of new facilities, additions to facilities, and facility renovations.

f. When an incident occurs in which an asset is compromised.

2.2.5. The physical security vulnerability risk assessment shall be conducted jointly by the Center security office and designated representatives of the using organization.

2.3 Implementation of Physical Security Vulnerability Risk Assessments

2.3.1. Based on the physical security vulnerability risk assessment results, the organizational head, in coordination with the Center Chief of Security, shall implement security measures described in the chapters found in this NPR, as appropriate.

2.3.2. Implemented physical security and terrorism counteraction measures shall be recorded in writing. Copies of these records shall be maintained by the Center Chief of Security and the organization concerned.

CHAPTER 3: Physical Security Requirements for NASA Assets by Category

3.1 General

3.1.1. This chapter classifies common types of NASA property in readily understandable categories for quick reference.

3.1.2. Paragraphs 3.2. through 3.19 outline physical security and terrorism counteraction measures for specific categories of property by security risk level established using the risk assessment procedure in NPR 1620.2, Physical Security Vulnerability Risk Assessment.

a. Risk Level I physical security measures are considered as minimums.

b. Required physical security measures are designed to mitigate threats related to theft, potential compromise, damage, and sabotage of an asset resulting in temporary or permanent loss of the asset.

c. Additional terrorism counteraction measures are designed to mitigate terrorist threats related to the killing of people or the destruction of an asset.

3.1.3. For those assets where Risk Level I physical security measures have not been provided, the protection of the asset has only been considered at the higher level of risk based on its criticality to NASA's mission.

3.1.4. Chapter 4 of this NPR outlines physical security measures for other specified non-critical categories of property.

3.1.5. Although the asset categories of NASA property described in Chapter 4 does not necessarily require the conduct of a physical security vulnerability risk assessment, risk factors, property vulnerability, and appropriate protective measures shall be considered and employed where circumstances warrant.

3.1.6. Unless otherwise specified, perimeter fencing shall meet standard minimum requirements established in Chapter 6, section 6.6.

3.1.6.1. Modifications to interior physical security fences shall not be made solely to conform to the requirements of this NPR if the existing fence provides a comparable deterrent to penetration, and other compensatory measures, including electronic monitoring and sensing equipment are incorporated, where appropriate.

3.1.6.2. Installation perimeter fences not meeting the standard requirements established in Chapter 6, section 6.6, shall be properly prioritized for replacement by Center management based on the criticality of the asset, its level of vulnerability, and any reasonable and sustainable compensatory security measures that, when implemented, reduce the vulnerability to manageable levels.

Otherwise, the fence must be replaced at the earliest possible time, but not to exceed 24 months from time of determination.

3.1.7. For assets situated off NASA Centers, or in foreign countries, physical security measures outlined in Chapter 1, section 1.3 shall apply, at a minimum.

3.1.8. In those instances where physical security lighting is required, current national industry requirements, as established by the Illuminating Engineers Society of North America (IESNA), shall be consulted as a guide in deciding lighting patterns and minimum protective lighting intensities and requirements.

3.1.9. The CCS shall ensure requirements for electronic access control systems, intrusion detection systems (IDS), closed circuit television (CCTV), and other types of electronic physical security systems are coordinated with the Office of Security Management and Safeguards, to ensure appropriate systems integration and Agencywide system operations capability.

3.1.10. Conflicts between security and safety requirements must be identified and resolved in writing. Every effort shall be made to accomplish implementation of physical security requirements while ensuring safety issues are appropriately addressed. Waiver or exception requests must be processed jointly by the Center Security and Safety Offices in accordance with Chapter 1, paragraph 1.3, of NPR 1600.1, NASA Security Program Procedural Requirements.

3.2 Categories of NASA Physical Assets

3.2.1. A NASA asset may not always correspond exactly to the categories listed in paragraphs 3.3 through 3.17. If the identified asset does not fall within one of the categories listed in table 2-1, NPR 1620.2, Physical Security Vulnerability Risk Assessment, or if it falls within more than one category, select the category which most closely describes the asset, and note the difference in the asset description. If none is appropriate, the organization head, in conjunction with the CCS, shall develop and carry out those physical security measures deemed appropriate to safeguard the asset.

3.3 Aircraft and Components at NASA Aviation Facilities (Includes Remotely Piloted UAV and balloons)

3.3.1. Risk Level I.

a. When not in use, aircraft and aircraft components; to include crewmember equipment, at NASA aviation facilities, shall be placed in the most secure hangars or structures available on the Center.

b. When aircraft are not stored in storage structures, and when operational requirements permit, keep aircraft adequately separated from each other to limit potential for multiple aircraft incidents, but close enough for ease of monitoring, and away from the perimeter of the aircraft parking area.

c. Unless otherwise specified, aviation facility aircraft parking/ramp areas and runways shall be protected by a standard perimeter physical security fence as described in Chapter 6, Section 6.6.

d. Each NASA aviation facility shall develop, maintain, and update a written physical security plan. Aviation facilities located on other than NASA property shall coordinate the physical security plan with the appropriate host authorities. A copy of the physical security plan shall be provided to the CCS.

e. Each NASA aviation facility shall appoint a Facility Security Manager who shall work with the CCS to ensure security concerns are properly addressed and required measures implemented.

f. For aircraft parked at NASA aviation facilities where guards or roving patrols are available, aircraft shall be checked at least every 4 hours.

g. Access to aviation facility aircraft and aircraft components shall be controlled at all times. At a minimum, the airfield shall be designated and posted as a "Restricted" area.

h. Unescorted access to aviation facilities, aircraft, or ramp space/taxiways shall be authorized only after completion of an appropriate background investigation, attendance at a Center aviation safety briefing and subsequent issuance of an appropriate Airfied access photo-ID. [Note: No visible designator (letter, logo, etc.) will be placed on the face of the individual's official NASA photo-ID.]

i. Privately-owned vehicles shall be prohibited from the flight line or other areas where aircraft are parked, except when authorized in writing, by the aviation facility or airfield manager and CCS.

j. Aviation facility auxiliary power units for starting aircraft, vehicle tugs, forklifts, aircraft boarding ladders, and other items that might be used to circumvent existing physical security measures shall be secured during non-duty hours to prevent unauthorized use.

k. Unidentified luggage, parcels, etc. shall not be placed on aircraft until adequately screened or the owner is identified. All unclaimed luggage, etc., shall be turned over to security personnel for appropriate disposition.

l. Visitors (U.S. citizen and foreign nationals) shall be escorted at all times.

m. Foreign National contractor employees shall be properly cleared in accordance with NPD 1371.5 and NPR 1371.2. Escort requirements shall be in accordance with Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.3.2. Risk Level II.

a. All measures required for Risk Level I shall be implemented.

b. Aviation facility aircraft parking areas shall be protected by a standard perimeter physical security fence equipped with vehicle barrier cabling and other equipment (e.g., jersey barriers) capable of defeating or delaying incursions by bomb-laden vehicles.

c. Entry to and exit from all buildings associated with the aviation facility, aircraft parking areas, and support equipment storage areas shall be controlled at all times. Entry and exit can be controlled through manpower and procedural means, mechanical means, or electronic means.

3.3.3. Risk Level III.

a. All measures required for Risk Levels I and II shall be implemented.

b. Aviation facility aircraft parking areas shall be lighted at night sufficiently to allow physical security personnel to detect intruders. Airfield lighting shall be coordinated with the aviation facility manager for consideration of safety and training issues.

c. Where threat circumstances warrant, airfield perimeter physical security fencing shall be equipped with a perimeter intrusion detection system designed to alert a monitoring station to suspicious activity.

d. Where threat and/or mission circumstances warrant, IDS and CCTV shall be added to hangars where aircraft are stored.

e. Security Officers shall provide continuous roving surveillance of aircraft parked at NASA

aviation facilities. Aviation unit personnel working on or near aircraft may be considered to be equivalent to continuous surveillance provided appropriate emergency duress procedures are available to ensure timely notification and response by security officers. CCTV and IDS may be installed as an alternative to providing continuous surveillance for outside aircraft.

f. Aircraft and hangar areas shall be checked on a random basis by armed security personnel.

3.4 NASA Aircraft and Components Not at NASA Aviation Facilities

3.4.1. At a minimum, Physical Security Protective Measures for Risk Level I in subparagraph 3.3.1 above shall be implemented. In addition, the physical security procedures indicated below shall apply:

a. Aircraft shall be parked, whenever practical, at a Government airfield or civilian airport with an active physical security program. If a location has no security program and a crewmember cannot remain with the aircraft, the aircraft commander shall advise aviation facility and local law enforcement authorities, as appropriate, of the aircraft location, identification, length of stay, and ways to contact crewmembers.

b. The aircraft shall be checked at least once daily by a crewmember for any evidence of tampering, sabotage, placement of explosive devices, and loss or damage to aircraft or mission components.

c. When utilized for Ferry Flight operations, the Shuttle Carrier Aircraft shall be provided with physical security measures as identified in the KSC Security Handbook (KHB 1610.1) and DDMS FUNCPLAN 3610.

3.4.2. When appropriate, accessible and easily removable components shall be removed and stored in a location capable of being secured against theft, sabotage, or vandalism.

3.5 NASA Vehicles and/or Watercraft and Components

3.5.1. When not in use, vehicles shall be parked in motor pools to the maximum extent practicable. The motor pool shall be protected by a standard physical security perimeter fence or adequately monitored to preclude theft or vandalism. Watercraft shall be secured to docking facilities.

3.5.2. Risk Level I. Vehicles parked on the installation or watercraft docked at docking facilities shall be secured with a locking mechanism. These vehicles/watercraft shall be locked as follows:

a. Commercially-designed vehicles. Activate manufacturer installed door and ignition locking device(s).

b. Non-commercial-design vehicles/watercraft. Immobilize steering wheel with a chain and a U.S. Government approved padlock as specified in local policies. Activate installed door and ignition-locking devices. Hood, spare tires, and fuel tank shall also be secured with approved locking devices if the local environment warrants this action. High-security padlocks supplied with vehicles may be used to secure vehicles as long as other physical security measures required by applicable directives are followed.

c. Material handling equipment. Material handling equipment (MHE) and other NASA vehicles that cannot be secured as indicated in (a) and (b) above shall have the steering mechanism immobilized or transmission lever locked in the neutral position. Alternatively, these vehicles may be stored in secure structures.

d. Signs. "Off Limits To Unauthorized Personnel" signs shall be posted at the activity entrances.

e. Where guards or roving patrols are available, motor pools and docking areas shall be checked for tampering, sabotage, loss, and damage not less than once every 4 hours.

f. Privately-owned vehicles shall not be permitted in motor pools except those of organizations and personnel engaged in deployments. These persons may store privately-owned vehicles in the motor pool at the discretion of the Center Director or his/her designee, provided physical security measures are taken to safeguard NASA vehicles and components remaining in the motor pool.

3.5.3. Risk Level II.

a. All measures required for Risk Level I shall be implemented.

b. Vehicle parking areas, except those for empty trailers, and watercraft docking facilities, shall be lighted during the hours of darkness.

c. Vehicles shall be parked at least 20 feet from the perimeter of the parking area or as far from the perimeter as possible.

d. Entry to and exit from motor pools and docking facilities shall be controlled. Control of entry and exit may be by guards or locks on gates. Organization personnel working within the motor pool or on the dock may be considered an alternative to guards.

e. Types of vehicles particularly vulnerable to theft, misappropriation, or damage in the motor pool, shall be segregated. These vehicles shall be placed where organizational personnel can see them during operating hours and where roving guards can see them during non-operating hours.

f. Guards shall conduct physical security checks on the motor pool and/or docking facility on an irregular basis, but not less than once every 2 hours.

3.5.4. Risk Level III.

a. All measures required for Risk Levels I and II shall be implemented.

b. Ground anchors shall be constructed for trailers, semi-trailers, and other towed equipment or a cable shall be run through all items of such equipment and a lock shall be affixed to one end.

c. Vehicles particularly vulnerable to theft, misappropriation, or damage shall be placed in secured garages and motor sheds to the maximum extent practicable.

d. The motor pool/docking facility shall be designated a "restricted" area.

e. Personnel must have written authorization from organization heads or designee, before vehicles/watercraft are dispatched.

f. Operators shall be checked for possession of a valid operator's permit by motor pool or dock personnel, or guards before they use the vehicle or watercraft.

g. Continuous surveillance shall be made of the motor pool/docking facility by armed guards.

h. CCTV and other detection equipment may be installed as an alternative to providing continuous surveillance by armed guards.

3.5.5. Exceptions. Exceptions to this policy are as follows:

a. Vehicles/watercraft actively employed in field operations, or pending turn-in through property

disposal channels.

b. Dispatched emergency, security police, courtesy patrol, and interior guard vehicles/watercraft for brief periods when response time is critical for the successful performance of operator or crew duties. Ignition keys shall be removed from unaccompanied vehicles.

c. Trailers, semi-trailers, towed trailer systems, and other non-self-propelled vehicles.

d. Inoperable, unserviceable vehicles/watercraft. Procedures shall be implemented to protect these vehicles/watercraft from cannibalization, vandalism, etc.

e. Vehicles/watercraft without installed locking mechanisms, under the continuous surveillance of a guard or located in a secure location.

f. NASA vehicles outside the United States when so designated by the project manager.

g. Fuel tanker vehicles when, in the judgment of management personnel or the CCS, locking would create a potential unacceptable hazard to life or property. In this case, compensatory security measures, established jointly by the CCS and management, shall be taken.

h. Accessible and easily removable components. These components, vulnerable to theft because of value or utility, shall be removed and secured separately. Additional physical security for components shall be provided by one of the following methods:

(1). Storing in a securable storage structure.

(2). Storing in a locked, totally enclosed truck or van.

(3). Storing in a locked equipment box or similar container secured to an open bed vehicle; for example, in a locked toolbox chained to the bed of a truck.

(4). Securing the item directly to the vehicle by a locally fabricated method.

i. Master-keyed locksets. Use of master-keyed locksets to secure NASA vehicles or motor pools are prohibited except under the following conditions:

(1). When the lockset is used within one vehicle to secure the vehicle and its' various storage compartments. Master-keyed locksets shall not be used to secure more than one vehicle.

(2). When the lock-set is used to secure the manifold access doors and hatches of petroleum, oil and lubricants (POL) trucks (one set per truck) and, if they have hardened steel shackles, for the storage compartments of wreckers, heavy equipment, etc. (one set per vehicle). The same set shall not be used on more than one vehicle. Master-keyed locks shall not be used to secure vehicle steering wheels.

j. Keys and locks. Keys and locks shall be controlled according to Chapter 5, of this NPR.

k. Items used to defeat security measures. Items that can be used to defeat physical security measures, such as bolt cutters, hacksaws, oxyacetylene torches, axes, or steel rods or bars, shall be secured in respective tool kits or other secure locations when not in use.

3.6 NASA Vehicles, Watercraft, or Aircraft with On-Board Classified or Sensitive Equipment

3.6.1. NASA vehicles or aircraft with CONFIDENTIAL or SECRET components or equipment mounted either internally or externally on the vehicle or aircraft; located on NASA installations or

facilities, shall be secured with Risk Level II physical protective and physical security procedural measures established in paragraph 3.3, above.

3.6.2. When located at other than NASA owned and operated facilities, NASA vehicles or aircraft with CONFIDENTIAL or SECRET components or equipment mounted internally or externally shall be secured with at least the minimum physical security measures. These vehicles and aircraft shall be guarded at all times by an appropriately cleared and armed crewmember or dedicated armed guard.

3.6.3. NASA vehicles or aircraft with TOP SECRET components onboard shall be under constant surveillance by appropriately cleared and armed personnel regardless of location.

3.6.4. Equipment or components shall not be removed from vehicles or aircraft solely to fulfill a secure storage requirement. Frequent removal may cause increased equipment maintenance and may degrade operational readiness. However, classified equipment or components that can be readily dismounted without probable damage shall be dismounted and placed in secure storage, meeting local requirements established by the CCS.

3.6.5. In environments or unusual circumstances not clearly defined as requiring specific physical security measures under this NPR, the Center Chief of Security (CCS) shall establish appropriate physical security measures to protect the classified equipment or components.

3.6.6. Non-cleared personnel, cleared personnel with no "need to know," and foreign nationals, shall not be given access to classified or sensitive information or equipment without proper coordination with the appropriate Center Security personnel.

3.7 Petroleum, Oils, Lubricants (POL) at Bulk Storage Facilities

3.7.1. Risk Level I.

a. When not under the surveillance of personnel authorized to dispense the products, POL pumps shall be locked and electrical power shall be turned off. The electrical power shutoff shall be secured. Hoses to pumps shall be secured to prevent loss of POL through gravity feed. These measures are not required if pumps are activated by a credit card or key prompt type device.

b. Packaged POL shall be stored in structures capable of being secured against unauthorized entry. Large POL packages (for example, 55-gallon drums) shall be stored to preclude their use as hiding places for pilfered items.

c. Written instructions to POL-dispensing personnel shall include procedures for determining if patrons entering the facility are authorized.

d. When unattended, the facility shall be checked at least once every 4 hours.

e. POL credit cards, identification plates, and aviation fuel plates shall be centrally controlled.

f. Privately-owned vehicles shall not be permitted in POL storage facilities.

g. All issues of fuel shall be accounted for and supervised by authorized personnel.

h. Hoses or other devices to siphon fuel shall be secured. All containers that can be used to carry fuel also shall be secured.

i. Containers storing used POL shall be marked and stored separately.

j. Keys to POL storage areas, equipment, and buildings shall be controlled per Chapter 5 of this NPR.

3.7.2. Risk Level II.

a. Measures required for Risk Level I shall be implemented.

b. Storage facilities shall be bound by a standard perimeter physical security fence.

c. Gates and openings shall be closed and locked when not used.

d. "Off Limits to Unauthorized Personnel" signs shall be posted at the perimeter.

e. Facility attendants shall verify all POL quantities issued by personally reading the meter.

f. When unattended, the facility shall be checked at least once every 2 hours.

3.7.3. Risk Level III.

a. Measures established for Risk Levels I and II shall be implemented.

b. Storage facilities shall be lighted during the hours of darkness.

c. Seals shall be placed on all points of fuel storage that may allow extraction of fuel by any means. A broken seal may indicate tampering.

d. The storage facility shall be designated a "Restricted area."

e. Continuous surveillance shall be made of the facility by guards.

f. Intrusion detection systems and/or CCTV may be installed as an alternative to continuous surveillance by guards.

3.7.4. POL not at bulk storage facilities.

Risk Level I Physical Security Protective Measures and security procedures in subparagraph 3.7.1 above, shall be implemented. In addition, the following security procedures shall be implemented:

3.7.4.1. POL tank trucks that contain fuel and that are not under the surveillance of the operator or a dedicated guard force shall have:

a. Locked hatch covers where possible.

b. Locked manifold access doors.

c. Each manifold valve shall be secured with a transportation seal if a manifold access door cannot be locked.

d. Approved padlocks as specified (e.g., non-sparking brass locks for safety), if available.

e. Fuel pods on vehicles and fuel vehicle tanks shall be secured with approved padlocks when the vehicles or tanks are carrying fuel and are not under the surveillance of the operator.

f. Fuel-carrying vehicles shall be parked in lighted areas of airfields or in motor pools protected by locked perimeter barriers or guards, whenever possible.

g. Dome covers and manifold system shutoff valves of tanker rail cars with POL products aboard shall be locked when they are located on an installation for unloading and when POL handling personnel do not have the equipment under surveillance. Rail cars with packaged POL products aboard shall be secured by locking all doors.

h. Packaged POL not onboard a vehicle or rail car shall be safeguarded in such a manner as to preclude theft or tampering. To increase the security posture above minimum the area may be

protected by security lighting, perimeter fence, guards, or IDS. The need for implementing these additional measures shall be determined by local threat and vulnerability assessments.

3.8 Spacecraft Launch and/or Mission Control Facilities

3.8.1. Risk Level I.

There are no Risk Level I physical security protective measures for this type of asset.

3.8.2. Risk Levels II and III.

a. The facility shall be designated a "Limited Area" as a minimum designation.

b. A photo-ID system shall be used to identify authorized personnel.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, NASA Construction of Facilities Procedural Requirements, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements when other less costly compensatory measures could be implemented.

d. Access to the facility shall be controlled at all times via armed guards or the installation of a centrally managed access control system. An IDS/CCTV system shall be installed/integrated to ensure personnel accountability during all hours of activity, and to allow for real-time assessment of suspicious events.

e. The exterior of the facility shall be appropriately lit during the hours of darkness to allow security patrols the opportunity to detect unauthorized personnel and enhance CCTV operations.

f. Fence perimeter intrusion detection shall be utilized for all Risk Level III assets and for those Risk Level II assets that are not housed within a typical structure (i.e., electrical sub-stations or outside storage area for the asset). The perimeter IDS shall be placed so as to give the earliest indication of an intruder.

g. The facility shall be surrounded by a perimeter fence at a distance from the facility of at least 50 feet.

h. Clear zones of 30 feet on the inside and outside of perimeter fences shall be maintained.

i. Risk Level III assets shall be provided perimeter CCTV. The CCTV may be equipped with motion detection capability and utilized as a perimeter intrusion detection system as required by paragraph (d) above. Otherwise, the CCTV shall be integrated with the perimeter intrusion detection capability to provide immediate visual assessment of all alarm events.

j. IDS shall be deployed on all perimeter doors. First floor windows shall have glass breakage sensors, and all windows shall be locked regardless of floor.

k. All visitors (U.S. citizen and foreign national) shall be escorted, if facility is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), as established in Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

l. If facility is not part of the NASA MEIPP, escort of visitors shall be according to Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

m. Foreign National contractor employees shall be properly screened and managed in accordance with NPD 1371.5, Coordination and Authorization of Access by Foreign Nationals and U.S. Citizen Representatives of Foreign Entities to NASA, NPR 1371.2, Procedural Requirements for Processing

Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities, and Chapter 4, paragraph 4.14, NPR 1600.1, prior to accessing the facility.

3.9 Communication Facilities and Associated Equipment (Includes Tracking Stations)

3.9.1. Risk Level I.

There are no Risk Level I physical security protective measures for this type of asset.

3.9.2. Risk Level II and III.

a. The facility shall be designated a "Restricted Area."

b. A photo-ID system shall be used to identify authorized personnel.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements, when other compensatory physical security measures could be implemented.

d. Access to the facility shall be controlled at all times via the installation of a centrally managed and monitored access control system. An IDS/CCTV system shall be installed/integrated to ensure personnel accountability during all hours of activity and to allow for real-time assessment of suspicious events. Vehicle entry points shall be controlled at all times by armed guards trained and capable of responding to and appropriately managing all types of security incidents.

e. A standard perimeter physical security fence shall be installed around the facility and operational areas to ensure unauthorized personnel are kept away from the facility and operations areas.

f. The exterior of the facility shall be appropriately lit during the hours of darkness to allow security patrols the opportunity to detect attempts to breach the protected area.

g. Vehicle barriers (e.g. bollards, jersey barriers, etc.) shall be employed, as appropriate, to ensure the facility is adequately protected against approaches by bomb-laden vehicles.

h. All visitors (U.S. citizens and foreign nationals) shall be escorted, if the facility is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), established per Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

i. If the facility is not part of the NASA MEIPP, escort of visitors (U.S. citizens and foreign nationals) shall be according to local policy.

j. Foreign national contractor employees shall be properly managed in accordance with NPD 1371.5 and NPR 1371.2 prior to accessing the facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.10 Super - Computing Facilities and Data Centers

3.10.1. Risk Level I.

There are no Risk Level I physical and procedural security protective measures for this type of asset.

3.10.2. Risk Level II and III.

a. The facility shall be designated a "Restricted Area" as a minimum designation.

b. A photo-ID system shall be used to identify authorized personnel.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements when other compensatory measures can be implemented.

d. Access to the facility shall be controlled at all times via a centrally managed access control system. An integrated IDS and CCTV system shall be installed to ensure personnel accountability during all hours of activity, and to allow for real-time assessment of suspicious events.

e. The exterior of the facility shall be appropriately lit during the hours of darkness to allow security patrols the opportunity to detect unauthorized personnel and to enhance CCTV capability.

f. Vehicle barriers (e.g. bollards, jersey barriers, etc.) shall be employed, as appropriate, to ensure the facility is adequately protected against approaches by bomb-laden vehicles.

g. All visitors (U.S. citizens and foreign nationals) shall be escorted if facility is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), as established in Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

h. If facility is not part of the NASA MEIPP, escort of visitors (U.S citizen and foreign national) shall be according to local policy.

i. Appropriate fire-suppression systems, protected air systems, emergency power on/off controls, dedicated back-up power, emergency gas and water shut-off valves should be installed, as deemed necessary, based on local threat conditions.

j. Foreign national contractor employees shall be properly screened in accordance with NPD 1371.5 and NPR 1371.2 prior to accessing the facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.11 Facility Engineering Supply and Construction Material Storage Areas

3.11.1. Risk Level I.

a. Buildings storing supply and portable construction material shall be securable against unauthorized entry.

b. Outside storage areas shall be enclosed by a perimeter fence.

c. "Off-Limits to Unauthorized Personnel" signs shall be posted at facility entrances.

d. Access to the facility and to keys, padlocks, and protective seals protecting access shall be controlled in accordance with Appendix I, NPR 1600.1, NASA Security Program Procedural Requirements.

e. Supplies shall be issued only to authorized personnel.

f. Incoming shipments of supplies shall be checked for improvised explosives devices (IED's).

g. Work orders shall be reviewed to determine if the recipient has requested excessive supplies for

the job to be done.

h. Entry of privately-owned vehicles into the storage building or outside storage areas shall be prohibited.

i. Entry of unchecked packages into the storage area shall be prohibited.

3.11.2. Risk Level II.

a. Measures required for Risk Level I shall be implemented.

b. Portable and easily pilferable items shall be separated from other supplies and construction material and stored in a separate room, building, or container with controlled access.

c. Outside storage areas shall be lit during the hours of darkness.

d. Small and easily pilferable supplies, construction material, and other items showing unexplained inventory loss shall be inventoried once each month. A copy of the inventory shall be kept until the next inventory.

e. Bulk packaged items securely crated, banded, or sealed shall remain in their original configuration and not broken until they are issued.

3.11.1.3. Risk Level III.

a. Measures required for Risk Levels I and II shall be implemented.

b. Buildings storing supplies and portable construction material shall be lit during the hours of darkness.

c. An IDS shall be installed in the storage building, if it is fully enclosed.

d. Landscaping features greater than 1 foot in height and other features that may obstruct views around the facility and provide concealment for aggressors shall be eliminated within 20 feet of the facility.

e. Access to storage areas shall be limited to facility personnel authorized to issue stock.

f. The storage building and outside storage areas shall be checked at least every 2 hours by a roving guard during hours that the facility is not operational.

3.12 Rocket Engine, Wind Tunnels, Simulators, and Other High-Speed Testing Facilities and Equipment

3.12.1. Risk Level I.

There are no Risk Level I physical and procedural security protective measures for this type of asset.

3.12.2. Risk Level II and III.

a. The facility shall be designated a "Restricted Area," as a minimum designation.

b. A photo-ID system shall be used to identify authorized personnel.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements when other compensatory measures could be

implemented.

d. Outside testing facilities shall be surrounded by a physical security fence meeting the minimum requirements stated below:

(1). Unless otherwise specified, interior perimeter fencing shall meet standard minimum requirements as established in Chapter 6 of this NPR.

(2). Modifications to existing interior perimeter fences shall not be made solely to conform to the requirements of this regulation if the existing fencing provides a similar deterrent to penetration, and other compensatory measures, including electronic monitoring and sensing equipment are incorporated, where appropriate.

e. Access to the facility shall be controlled at all times via armed guards or the through installation of access control systems. An IDS/CCTV system shall be installed/integrated to ensure accountability during all hours of activity and to allow for real-time assessment of suspicious events.

f. The exterior of the facility shall be appropriately lit during the hours of darkness to allow security patrols the opportunity to detect unauthorized personnel, and to enhance CCTV capability.

g. All visitors (U.S. citizens and foreign nationals) shall be escorted if facility is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), as established in Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

h. If the facility is not part of the NASA MEIPP escort of U.S. citizen and foreign national visitors shall be according to local policy.

i. Foreign national contractor employees shall be properly screened in accordance with NPD 1371.5 and NPR 1371.2 prior to accessing facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.13 Research and Associated Facilities

3.13.1. Risk Level I.

a. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements, when other compensatory measures could be implemented.

b. Facilities shall be locked during non-duty hours to preclude unauthorized entry.

c. The exterior of the facility shall be appropriately lit during the hours of darkness, to allow security patrols the opportunity to detect unauthorized personnel.

3.13.1.2. Risk Level II and III.

a. All measures for Risk Levels I shall be implemented.

b. The facility shall be designated a "Restricted Area," as a minimum designation.

c. A photo-ID system shall be used to identify authorized personnel.

d. Access to the facility shall be further controlled at all times via the installation of access control systems. An IDS/CCTV system shall be installed/integrated to ensure accountability during all hours of activity and to allow for real-time assessment of suspicious events.

e. All visitors (U.S. citizens and foreign nationals) shall be escorted if facility is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), in accordance with Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

f. If facility is not part of the NASA MEIPP, escort of U.S. citizen visitors only shall be according to local policy.

g. Foreign national contractor employees shall be properly cleared in accordance with NPD 1371.5 and NPR 1371.2, prior to accessing the facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.14 Animal Research Facilities and Associated Laboratories

3.14.1. Risk Level I.

There are no Risk Level I physical security protective measures for this type asset.

3.14.1.2. Risk Levels II and III.

a. The facility shall be designated a "Restricted Area," as a minimum designation.

b. A photo-ID system shall be used to identify authorized personnel.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements, when other compensatory measures could be implemented.

d. Access to the facility shall be controlled at all times through the installation of a centrally managed access control system. An IDS/CCTV system shall be installed/integrated to ensure accountability during all hours of activity and to allow for real-time assessment of suspicious events.

e. The exterior of the facility shall be appropriately lit during the hours of darkness to allow security patrols the opportunity to detect unauthorized personnel and to enhance CCTV capability.

f. All visitors (U.S. citizens and foreign nationals) shall be escorted, if facility is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), as established in Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

g. If facility is not part of the NASA MEIPP, escort of U.S. citizen visitors only shall be according to local policy.

h. Foreign national contractor employees shall be properly cleared in accordance with NPD 1371.5 and NPR 1371.2, prior to accessing the facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.15 Spacecraft (Shuttle, ISS, Etc.) and Associated Equipment

3.15.1. Risk Level I.

There are no Risk Level I physical security protective measures for this type of asset.

3.15.2. Risk Level II and III.

a. Asset shall be isolated from the general public.

b. The asset shall be designated a "Restricted Area," as a minimum designation.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible. Existing facilities shall not be retrofit to meet these requirements, when appropriate alternative compensatory security measures could be implemented.

d. While on a launch pad, the asset shall be protected by a perimeter physical security fence capable of preventing access. The area shall be well lit.

e Access to the facility and spacecraft shall be controlled at all times by armed personnel or the installation of a centrally managed access control system.

f. An IDS/CCTV system shall be installed/integrated to ensure accountability during all hours of activity, and to allow for real-time assessment of suspicious events.

g. While in transit to and from maintenance facilities and launch pads, the spacecraft shall be escorted by armed guards at a minimum.

h. All visitors (U.S. citizens and foreign nationals) shall be escorted, if facility or asset is included as part of the NASA Mission Essential Infrastructure Protection Program (MEIPP), as established in Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

f. If facility or asset is not part of the NASA MEIPP, escort of U.S. citizens and foreign national visitors shall be according to local policy.

g. Foreign national contractor employees shall be properly cleared in accordance with NPD 1371.5 and NPR 1371.2 prior to accessing facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.15.3. Terrorism counteraction measures specifically for NASA Spacecraft

Launch Operations.

3.15.3.1. NASA Spacecraft, most notably the Shuttle Transport System (STS) and future spacecraft, are NASA's most recognizable physical assets and as such are a potential target of terrorist intent on attacking the prestige of the United States . Launch preparations shall, at a minimum, include the following:

a. Long and short-term analysis of intelligence information for indications of specific threats directed against the Launch Vehicle.

b. Development and implementation of written security operation plans for each launch.

c. Continuous evaluation of status of key personnel (astronauts, families, launch/mission control personnel, etc.), to ensure appropriate levels of protection are in place and effective.

3.15.3.2. On-site and in-transit protection and accountability for Shuttle program components (e.g., solid rocket boosters, external tanks, etc.) shall be coordinated with the appropriate contractor organization, to ensure the level of protection afforded is commensurate with the threat and vulnerability determination.

3.16 Industrial and Utility Facilities and Equipment

3.16.1. Risk Level I.

a. Access into the area where the equipment is located shall be controlled to prevent unauthorized entry.

b. Keys to facilities and equipment shall be controlled per Chapter 5, NPR 1620.3, "Physical Security Requirements for NASA Facilities and Property."

c. The area shall be designated a "Restricted Area," as a minimum designation.

òá Risk Level II.

Measures for Risk Level I shall be applied and equipment shall be checked by roving patrols, at intervals not to exceed every 4 hours when the facility is unattended.

òá Risk Level III.

Measures for Risk Levels I and II shall be applied, except that checks by roving patrols, shall be every 2 hours when the facility is unattended.

3.16.4. Risk Level III.

a. If the equipment is not located within a structure, the area or vulnerable items of equipment shall be surrounded with an 8-foot-high reinforced concrete or masonry perimeter wall or surrounded by a physical security fence meeting the minimum requirements of Chapter 6, Section 6.6, of this NPR, and monitored by a centrally managed CCTV system.

b. If the equipment is located within a structure, the structure shall be equipped with a centrally monitored intrusion detection system (IDS).

3.17 Arms, Ammunition, and Explosives (AA&E)

3.17.1. At a minimum, AA&E, including pyrotechnics, shall be controlled/stored in accordance with the requirements in NPR 1600.1, NASA Security Program Procedural Requirements, Chapter 7, paragraphs 7.9.5 and 7.9.17, and 7.9.21 respectively. If deemed appropriate, Centers may adopt more stringent measures then those established in this NPR.

3.17.2. Organizations having access to and responsibility for AA&E, including pyrotechnics, shall establish strict accountability and inventory procedures. Procedures shall include:

(1) Issue and turn-in.

(2) Monthly inventory.

(3) Inspections.

(4) Proper storage and use of "shelf stock."

3.18 Mission-Critical and High-Risk Personnel

3.18.1. The NASA Assistant Administrator for Security Management and Safeguards, or his/her designee, in coordination with appropriate enterprise associate administrators, shall designate mission-critical and high-risk personnel.

òá Risk Level I.

Access to those areas of the facility where mission-critical and high-risk personnel are located shall

be controlled continuously when occupied.

òá Risk Level II.

a. Access to the entire facility shall be controlled continuously when occupied.

b. The exterior of the facility shall be appropriately lit during the hours of darkness, to allow security patrols the opportunity to detect unauthorized personnel.

3.18.4. Risk Level III.

a. Access to the entire facility shall be controlled at all times.

b. Access to the area surrounding the facility shall be controlled during times when the facility is occupied.

c. Specific threats shall be evaluated immediately by the Security Office and enhanced security provided, if determined appropriate.

d. Visitors to the facility who require entry into areas in which mission-critical or high-risk personnel are located shall be searched for weapons and explosives on at least a random basis.

e. Continuous surveillance of the area surrounding the facility shall be provided at all times, when the facility is occupied.

3.19 Administrative Support Facilities

3.19.1. Security procedural measures.

òá Risk Level I.

No such measures apply at this risk level.

3.19.1.2. Risk Level II and III.

a. Use of NASA photo-identification to facilitate entry of authorized personnel.

b. Use of a centrally managed electronic access control system and integrated video surveillance to facilitate access for authorized personnel and provide real time feed back on suspicious activity.

c. As appropriate to the situation, implement terrorism counter-measures identified in Section 3.20.

3.20 Terrorism Counteraction Measures

3.20.1. Terrorism counteraction measures.

3.20.1.1. Risk Level I.

a. Parking beneath facilities shall be eliminated where possible, and controlled where more practical to ensure only authorized personnel have access.

b. Parking exterior to the facility shall be kept as far away from the facility as possible, but at least 30 feet.

c. Trash receptacles, landscaping features, and other features greater than 1 foot in height that potentially provide concealment for aggressors or bombs shall be kept at least 50 feet from the facility.

d. Where feasible, locate mission-critical or high-risk personnel in the interior of the facility as far from the exterior as possible.

3.20.1.2. Risk Level II.

a. Windows into areas occupied by mission-critical or high-risk personnel shall be covered by a minimum 8-mil fragment retention film that shall be backed up by heavy drapes.

b. Windows and doors into areas occupied by mission-critical or high-risk personnel shall be locked such that any attempt to enter through them when the facility is unoccupied shall require forced entry, whose effects shall be noticeable.

c. Duress alarms shall be installed in areas occupied by mission-critical and high-risk personnel.

3.20.1.3. Risk Level III.

a. The facility shall be protected by a physical security fence meeting the minimum requirements of paragraph 3.1.6.2, at a distance from the facility of at least 50 feet.

b. Vehicle barriers (e.g., bollards, jersey barriers, etc.) shall be employed, as appropriate, to ensure the facility is adequately protected against approaches by bomb-laden vehicles.

á

CHAPTER 4: Minimum Physical Security Requirements for Other Categories of NASA Property Not Necessarily Subject to Risk Assessment.

4.1 Miscellaneous Pilferable Assets (Includes Hand-Held Precision Tools, Lap-top Computers)

4.1.1. Tool sets and kits with lockable toolboxes.

These items, when not in use, shall be secured with a U.S. Government approved key-operated tumbler-type lock, consisting of either a padlock (including brass padlocks issued with the tool boxes) or a factory installed built-in key-operated tumbler type lock. The individual who signed for the set or kit shall retain the key. A duplicate key may be held by the supervisor, if it is stored in a locked container with controlled access.

4.1.2 Portable hand tools (e.g., electronic tools, tool sets or kits, and shop equipment).

Portable hand tools, tool sets or kits, and shop equipment. These items, when not in use and not under the surveillance of a responsible person (user, tool room keeper), shall be stored in a secure location. Non-portable items shall be secured in the building or van in which they are located. Doors and windows shall be closed and locked. Secure locations for portable items include:

4.1.2.1. A locked building or room or a locked metal equipment cage in a secured building.

4.1.2.2. A locked built-in cabinet, bin, or drawer in a secure room or bilding.

4.1.2.3. A locked drawer or compartment of a furniture item (wall locker, desk, etc.) in a secure room or building.

4.1.2.4. Attached to the building structure with a 5/16-inch chain or equivalent cable and a low security padlock or permanently fastened to a working surface.

4.1.2.5. Locally fabricated, lockable racks that, when locked, prevent toolbox lids from being opened or individually placed larger tools from being removed.

4.1.2.6. A locked enclosed truck, van, or vehicle trunk.

4.1.3. Common tools and portable shop equipment (includes power tools).

These items, when not on hand receipt to a user, shall be controlled through a locally devised receipt, sign-in/sign-out log, or exchangeable tag system. Tool checks (metal disks that can be

stamped or etched with an employee's identification) are available through supply channels under national stock number (NSN) 9905-00-473-6336.

4.1.4. Access.

Access to tools and shop equipment shall be controlled to the maximum extent practical. If possible, access shall be limited to the user, the individual designated as responsible for items when not in use, and supervisory personnel.

4.1.5. Keys and locks used to safeguard tools.

Keys, locks, and protective seals used to safeguard hand tools, tool sets or kits, shop equipment, and the facilities in which they are stored or located shall be managed per Chapter 5 of this NPR. Master-keyed or keyed-alike lock-sets shall not be used to secure these items.

4.1.6. Special accountability.

Precision hand-tools that are made for a specific purpose, and are usually expensive to replace, shall be placed under special accountability. Consideration shall be given to marking these items for identification and accountability.

4.2 Administrative and Housekeeping Supplies and Equipment

4.2.1. Minimum physical security requirements for furniture and office equipment.

Office buildings or rooms in which these items are located shall be secured when no responsible member permanently assigned to that particular activity is present.

4.2.2. Minimum physical security requirements for office machines.

4.2.2.1. Buildings, rooms, and offices in which office machines are located shall be secured, whenever an individual permanently assigned to the activity is not present. Security shall consist of closing and locking appropriate doors and windows, as a minimum.

4.2.2.2. Automated systems, including word processing systems, shall be secured to preclude theft.

4.2.2.3. When size and weight allow, small office machines such as hand-held calculators and portable lap-top computers shall be locked in a desk or cabinet.

4.2.3. Minimum physical security requirements for expendable and consumable supplies.

4.2.3.1. At the office levels, items not issued for actual use shall be centrally stored in secure cabinets, containers, rooms, or buildings. Keys, locks, protective seals, and access to storage facilities shall be controlled.

4.2.3.2. Pilferable items (e.g., pens, pencils, etc.) shall be stored in a central supply closet or securable metal cabinet, and issued when needed.

4.3 Precious Metals/Materials

4.3.1. Physical Security Protective Measures.

Precious metals/materials shall be stored in secure containers within a locked room or a secure storage area. Large quantities shall be provided with additional protective measures, such as IDS and CCTV.

4.3.2. Security procedural measures.

4.3.2.1. Users of precious metals/materials shall establish an accountability system, if not required under other regulations, to properly control the metal/materials. The system shall include:

(a) Inventory log.

(b) Inspection process.

(c) Issuance and turn-in process.

4.3.2.2. The Offices of Security, Logistics, and users of precious metals/materials shall jointly conduct inspections of stocks to ensure storage, protection, and usage procedures are properly followed.

4.4 Mailrooms

4.4.1. Minimum physical security requirements for mailrooms.

4.4.1.1. Facilities housing these assets shall meet physical security requirements necessary to preclude unauthorized access. Existing facilities shall be retrofit to meet these requirements or other compensatory measures (e.g., access control system, IDS, etc.) implemented.

4.4.1.2. Installation of metal caging inside of a structure shall be considered for separation and control of mailroom areas.

4.4.2. Physical Security Measures.

4.4.2.1. Access to the mailroom shall be controlled at all times. Installation of an access control system is an alternative to managing access via personal recognition by mailroom personnel.

4.4.2.2. Installation of an intrusion detection system (IDS) is recommended for after-hours protection.

4.4.2.3. The exterior of the facility shall be appropriately lit during the hours of darkness, to allow security patrols the opportunity to detect unauthorized personnel.

4.4.2.4. The facility or room shall be designated a "Restricted Area," as a minimum designation.

4.4.2.5. In coordination with the CCS, the mail handling activity shall develop a mail security plan, as required under 41 CFR Part 101-9, Part 102-192.85.

4.4.2.6. A photo-ID system shall be used to identify authorized personnel.

4.4.2.7. Visitors shall be escorted at all times.

4.4.2.8. Mailroom operations shall include the use of package screening devices for explosives and chemical/biological agent detection. Any mail identified as suspect shall be reported immediately to security personnel.

4.4.2.9. Centers shall consider establishing a "centralized" shipping and receiving activity to preclude direct customer receipt of threatening or dangerous mail/packages.

4.4.2.10. Self-contained air-handling equipment shall be installed to ensure contaminated air is properly mitigated. Procedures shall be in place for local evacuation of the mailroom facility, and if applicable, the shutdown of the air handling equipment for the mailroom.

4.4.2.11. Where appropriate, Center safety and security organizations shall collaborate on all facility and equipment design aspects of mailroom construction or modifications, to ensure designs meet safety and security operational expectations commensurate with existing threats.

4.5 Security of Medical Supplies and Equipment at Medical Facilities

4.5.1. Security Policy

4.5.1.1. Facilities, vaults, and containers used for storage of controlled medical substances or medically sensitive items shall not be used for storage of classified material.

4.5.1.2. A Serious Incident Report shall be submitted per Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements, for significant theft, loss, or recovery of Government-owned or possessed narcotics, dangerous drugs, controlled substances, precious metals, radioactive or other sensitive materials, including sensitive medical material or equipment, or mismanagement of stock records or recovery procedures for those items that prevent a determination of loss.

4.5.1.3. Schedule I drugs and substances shall be secured in the same manner prescribed controlled substances.

4.5.2. Personnel who are assigned duties that require access to controlled medical substances and sensitive items storage areas, including volunteers or those who have custodianship or possession of keys and combinations to locks securing such areas, shall be carefully selected and appropriately screened per Chapters 3 or 4, NPR 1600.1, NASA Security Program Procedural Requirements.

4.5.2.1. Criteria for selection of these personnel shall include moral character, prior employment history, maturity, and trustworthiness. Prior to assuming these duties:

a. Designated persons shall have satisfactorily undergone a local records check (LRC). Personnel exhibiting financial irresponsibility shall be excluded from consideration. Non-Government workers (e.g., volunteer workers) shall not be given unsupervised access to controlled medical substances and sensitive items. For new Government employees, results of the required investigation shall be known prior to granting them unescorted access.

b. An interview, by an appropriate Center security official, with the lowest level manager having managerial responsibility for the security of subject items is required. The purpose of the interview is to appraise the individual's character, judgment, reliability, attitude, emotional or mental maturity, and sense of responsibility. The interview shall be documented in writing.

4.5.2.2. The names and duty positions of personnel authorized unaccompanied access to controlled medical substances and medically sensitive items storage areas shall be depicted on a roster, which shall be posted inside the storage area.

4.5.2.3. Access to controlled substances denied to individuals undergoing investigation, treatment, rehabilitation, judicial, or administrative action as a result of actual or suspected drug use may be reinstated when--

a. Suspicions or allegations against the individual are determined to be unfounded.

b. Rehabilitation is successful.

4.5.3. Physical security during shipments of controlled medical substances and medically sensitive items shall be per appropriate NASA directives. In any event, in-transit security must be such that

the requirements of this NPR are not violated and that controlled medical substances and medically sensitive items are protected from unauthorized possession, use, and theft.

4.5.4. Disposal of controlled medical substances and items shall be per the provisions of the appropriate NPD and NPR.

4.5.5. Controlled medical substances or sensitive medical items shall be stored in secure storage locations or in locked containers.

4.5.5.1. Containers shall be locked at all times, except during restocking, inventory, or dispensing operations.

4.5.5.2. As a minimum, storage shall be in a location designated as a "Restricted Area," and protection provided shall be consistent with the type of item and perceived local threat of theft or diversion to unauthorized use.

4.5.6. At the close of business, designated personnel shall perform a security check prior to departure from rooms or facilities in which controlled medical substances and sensitive medical items are stored. These security checks shall be documented daily on Standard Form 701, Activity Security Checklist, as a minimum. This form shall ensure that:

4.5.6.1. No controlled items remain unprotected or exposed and that they are secured in designated containers.

4.5.6.2. Security containers are locked and checked properly with such action recorded on an SF 702 (Security Container Check Sheet).

4.5.6.3. All windows, doors, and other openings are secured to deter access to rooms in which containers are located.

4.5.6.4. Other vulnerable equipment or property is stored properly and secured.

4.5.6.5. When the medical facility is not occupied, security checks shall be conducted by security patrols at irregular intervals, not to exceed every 4 hours to avoid establishing a pattern. An intrusion detection system may be installed, to augment security patrol checks.

4.5.6.6. If used, the IDS shall consist of at least two types of intrusion sensors, a means of alarm annunciation at a central monitoring location, from which an armed response force can be dispatched, and electronically supervised circuitry between the two.

4.5.6.7. If the substances are entirely within a container, detection may include a capacitance sensor on the container itself.

4.5.6.8. If the substances are not entirely within a container, IDS sensors shall be installed such that they detect intruders before they breach any components of the vault, room, or building that are associated with providing delay to the intruders. The vault, room, or building shall provide a delay greater than or equal to the time required for the response force to respond to the alarm.

4.5.6.9. Installation of IDS equipment shall be per applicable local specifications. When local conditions dictate, a duress switch or holdup button may be added. Design reviews apply.

4.5.6.10. An SOP for the activation, deactivation, and daily testing of the IDS shall be published by the security office. The SOP shall include instructions for maintaining an accurate IDS log.

4.5.7. All instances of suspected theft, loss, illegal entry, open or unlocked facilities or containers, and other incidents of a suspicious origin shall be reported immediately to designated authorities. Surveillance shall be maintained, until responding personnel arrive at the scene.

4.5.8. Storage areas shall be provided with operational interior and exterior lighting, at all times during the hours of darkness.

4.5.9. Medical Facility security coordinators shall establish procedures for the protection of locks, keys, and combinations used to secure facilities, vaults, and containers in which controlled medical substances and sensitive items are stored.

4.5.10. The number of people with access to keys and combinations shall be the minimum necessary for efficient operations.

4.5.11. Provisions listed in Chapter 5 of this NPR shall be followed in establishing key control procedures.

4.5.12. Clinics and veterinary (animal care) facilities shall conform to the physical security requirements listed below.

4.5.12.1. When duty personnel are in attendance 24 hours a day, normal operating quantities of controlled medical substances and sensitive medical items shall be stored in double-locked containers. Containers must be constructed so that forced entry is readily apparent to visual examination.

4.5.12.2. When duty personnel are not present 24 hours a day, normal operating quantities of controlled medical substances and sensitive medical items shall be stored in a GSA-approved safe and an additional barrier shall be provided, such as locating safes inside a locked room.

a. Normal operating quantities of controlled medical substances and sensitive medical items shall be stored according to the criteria in paragraph 4.5.12.1. above.

b. If this is not possible, containers constructed of a minimum of 26-gauge steel with a single lock may be used, provided additional security measures are taken (for example, increased surveillance or improved lighting), and provided the steel container is secured inside a locked room.

4.5.13. All storage containers for controlled medical substances and sensitive medical items shall be located in areas designated as "restricted" per Chapter 7, NPR 1600.1, NASA Security Program Procedural Requirements.

4.5.15. Containers shall be secured after duty hours.

4.5.16. To prevent loss or theft during operating hours, containers shall be unlocked only when property is being inserted, removed, or when the container is under the observation of designated personnel.

4.5.17. Unit dose carts containing controlled substances shall be kept in restricted areas when not in use.

4.5.18. To prevent loss or theft during the administration of medications, unit dose carts shall be kept under the physical control or unobstructed observation of designated personnel.

4.5.19. Storage areas shall be provided with operational interior and exterior lighting, at all times during the hours of darkness.

4.5.20. The number of crash carts and emergency trays (essential emergency assemblages) that contain controlled substances shall be kept to a minimum, and shall be provided with maximum security consistent with requirements for immediate availability.

4.5.21. When controlled medical substances or items are issued to emergency medical team

personnel assigned to ambulance or emergency vehicle response duties, the controlled substances or items shall not be stored in the vehicle while it is unattended.

4.5.22. Controlled substances and items must remain under control or observation of responsible personnel at all times and, shall be stored in restricted areas when possible.

4.5.23. Locking devices on emergency assemblages hinder immediate availability to controlled medical substances and sensitive items by medical treatment personnel, and shall not be used.

4.5.24. Appropriate sealing devices may be used to indicate tampering and to assist in inventory, but they must be easily opened without the use of a key, combination, or other time-delaying device.

4.5.25. Emergency assemblages containing controlled medical substances shall be sufficiently protected, but must not hamper ready and authorized visual inspection and immediate removal for use.

4.5.26. Accountability and control requirements are per applicable organization policy.

4.5.27. Unused needles, syringes, and other medically sensitive items shall be stored in a locked container.

4.5.28. Used and unused needles and syringes shall not be stored in the same cabinet or container.

4.5.29. Pending final destruction, used needles and syringes may be temporarily stored in closed one-way puncture resistant receptacles ("Sharps" containers).

4.5.30. "Sharps" containers must be of a tamper-resistant design, and must be either:

4.5.30.1. Locked to a mounting device that is securely fastened to the building structure.

4.5.30.2. Located in a room or area that is locked or under continuous visual surveillance of ward or clinic personnel.

4.6 NASA Visitor Centers and Outdoor Exhibit Displays

4.6.1. NASA Visitor Centers traditionally house one-of-a-kind, irreplaceable items of historical significance. Such items are generally considered invaluable because they are irreplaceable and shall be considered sensitive property. They shall be reasonably protected.

4.6.1.2. The degree of protection necessary must be determined locally and in partnership between the NASA COTR, Visitor Center Manager, Center Chief of Security, and supporting facility engineers.

4.6.1.3. Visitor Center buildings and apertures providing access to the building shall be modified or constructed so as to delay a determined intruder long enough for a security force to respond.

4.6.2. Security measures shall be implemented for those facilities and assets protected under the National Preservation Act of 1966 to the extent permitted. Consistent with this Act, IDS coverage shall be included for all vulnerable windows and doors.

4.6.3. Personnel assigned or attached (including special duty personnel) to staff NASA Visitor Centers must meet the security reliability requirements established in Chapter 4, NPR 1600.1, NASA Security Program Procedural Requirements.

4.6.3.1. At a minimum, a favorable National Agency Check (NAC) and local records check (LRC) shall be required by the Center Security Office before personnel are assigned or attached (including

special duty personnel) to Visitor Center duties.

4.6.4. The Visitor Center director, or designee, shall be designated the key custodian, whenever feasible.

4.6.5. Exterior doors used for access to Visitor Centers shall be secured with U.S. Government-approved padlocks (grade II, hardened steel shackle and body), deadbolt or other locks equal to these devices, as determined by the servicing facility engineer, if installation does not detract from the aesthetic value of the facility. The number of exterior doors with exterior exposed padlocks shall be kept to the absolute minimum. All other exterior doors shall be secured on the inside.

4.6.6. Visitor center keys shall be maintained separately from high-value item storage IDS keys.

4.6.6.1. Keys shall not be left unattended or unsecured at any time.

4.6.6.2. The use of a master or multiple key system shall be in accordance with Chapter 5 of this NPR.

4.6.7. Where a NASA Visitor Center or exhibit is protected by an approved IDS, and the IDS is operational, museum personnel, as authorized by the Visitor Center manager, may remove the keys to the Visitor Center or exhibit from the installation at which the Visitor Center or exhibit is located. Unless authorized by the Center Chief of Security (CCS), where an approved IDS is not installed, the Visitor Center keys shall not be removed from the installation, but shall be locked in a secure strongbox in a secured location on post, such as the security dispatch office. Visitor Center personnel, as authorized by the Visitor Center Manager, may retain custody of the keys in this strongbox.

4.6.8. Duplicate keys shall not be kept with operational keys. They shall be maintained by the Visitor Center manager, Center locksmith, or placed in a secure location where they may be accessed by authorized personnel only.

4.6.9. Where combination locking devices are used to secure items such as containers and display cases, the combination shall be controlled and safeguarded to preclude unauthorized access.

4.6.10. Interior and exterior lighting shall be provided in all Visitor Center buildings in which sensitive property is located. Lighting around artifacts shall have proper UV filtering for artifact conservation. Sensitive property is property requiring a high degree of protection and control because of its vulnerability to theft or potential for use in an illegal activity, or for its historic value. As a minimum, all entrances shall be lit during hours of darkness.

4.6.11. Installation of IDS may supplement existing security measures or provide a commensurate degree of protection. Established Center requirements for IDS and access control systems shall apply.

4.6.12. The viewing surfaces of exhibit or display cases shall be constructed of at least 1/4 inch-thick plate glass, transparent acrylic plastic, or transparent poly-carbonate plastic, securely fastened into frames or into the container. UV acrylic shall be used as appropriate to facilitate artifact conservation.

4.6.12.1. Where plate surfaces join at an angle, the edges shall be bonded and rounded to prevent insertion of a pry tool. UV acrylic shall be used as appropriate to facilitate artifact conservation.

4.6.12.2. Cases with hinged openings must have all hinge butts concealed or spot welded, or use a comparable security measure.

4.6.12.3. Non-viewing surfaces of cases shall be constructed to offer a higher degree of protection than the viewing surface.

4.6.13. Workshops used by museum personnel for maintenance or restoration work shall be secured at the close of each business day.

4.6.14. Each Visitor Center shall be attended by at least one member of the Visitor Center staff, who is tasked with Visitor Center security while it is open to the public. This function can be combined with other duties.

4.6.14.1. Visitor Centers that are organized within several separate, non-connecting buildings shall have Visitor Center or security personnel in each facility, an electronic monitoring system, or security personnel shall conduct periodic checks of facilities and displays.

4.6.14.2. The Visitor Center attendant shall be especially alert to detect pilferage, damage, or theft.

4.6.15. To ensure adequate surveillance of all parts of the Visitor Center, the installation of one-way mirrors and electronic sensing devices shall be considered and installed, as appropriate.

4.6.16. NASA Center Chiefs of Security (CCS) shall ensure that all Visitor Centers are on an assigned security patrol route, and that special orders include an unscheduled check at least once every 4 hours by that patrol during non-duty hours on a daily basis.

4.6.17. Large items of historical property that are displayed outdoors in Visitor Center parks shall be anchored to prevent theft.

4.6.17.1. Pilferable component parts shall be secured to the display or removed at the close of each business day.

4.6.17.2. Visitor Center parks and exterior displays shall be provided electronic and/or video surveillance where warranted, and checked periodically by security patrols.

4.6.18. Loss of historical property shall be reported to the security officer for appropriate investigation.

4.7 NASA Child Care Facilities

4.7.1. To the extent practical child care facilities shall be situated and constructed to ensure maximum protection of children and staff. Child care facilities shall not be situated adjacent to Center fence perimeters or critical infrastructure assets. Center security personnel shall be consulted during design processes to ensure appropriate security measures are included.

4.7.2. Retrofitting existing facilities to meet minimum security considerations established by this NPR is essential to offsetting any security vulnerabilities caused by construction deficiencies.

4.7.3. To ensure appropriate access control and personal accountability, NASA Centers shall employ IT-based access control systems at all child care facilities:

4.7.3.1. Center Security Offices shall ensure the installation of an IT-based duress (panic) system throughout the child care facility.

4.7.3.2. All rooms and outside play areas shall have duress capability. Child care staff shall be trained and periodically tested in the use of the duress system.

4.7.3.3. Use of CCTV to assist in management of security at NASA child care facilities is mandatory for outside play areas, facility and fence perimeter, reception areas, and other areas presenting

security concerns.

4.7.4. Security fencing shall be installed around all exposed play areas.

4.7.5. All entrance gates shall be secured and made capable of being opened from the inside only.

4.7.6. A key or access control card shall be required to open gates from the outside.

4.7.7. Minimum fencing characteristics shall be in accordance with the specifications outlined in Chapter 6 of this NPR, and additional requirements established below.

4.7.7.1. Playground equipment shall not be installed within 15 feet of a perimeter security fence.

4.7.7.2. Installation of "Privacy Slats" to preclude unauthorized outside surveillance.

4.8 TV, VCR, DVD, Cameras, Bicycles, and other Sensitive Items

Center management shall ensure items of value, as defined in NPR 4200.1E, NASA Equipment Management Manual, are provided protection commensurate with local theft conditions and accountability practices.

CHAPTER 5: Keys, Locks, Locking Devices (Including Hasps and Chains), and Protective Seals

5.1 Key Issuance

a. Keys shall be signed out to authorized personnel, as needed, on a key issue form.

b. Only authorized Government personnel, branch head or higher, and their designees, may approve the issuance of keys to organizational personnel for facilities under their control.

c. Keys for contractor personnel shall also be issued in accordance with paragraph b. above.

d. Office keys shall be issued to occupants of that office only.

5.2 Master Keys

a. Building master keys shall be kept to the absolute minimum.

b. No more than the minimum number of building master keys shall be issued, and then only to key personnel in that facility.

c. Center master keys shall be issued only to security, fire, and when appropriate, other authorized personnel.

5.3 Key Depository

a. A lockable container, such as a safe, filing cabinet, or a key depository made of at least 26-gauge steel, equipped with a tumbler-type or touch-pad locking device and permanently affixed to a wall, shall be used to secure keys.

b. The key depository shall be located in a room where it is kept under 24-hour surveillance or in a room that is locked when unoccupied.

c. The locksmith shop key and records storage area shall be protected by an Intrusion Detection System (IDS).

5.4 Locks

a. The use of a master key system or a multiple key system shall be strictly managed by the installation locksmith. Management of NASA-owned buildings shall not procure coring and keying

services of outside companies.

b. U.S. Government key-operated, pin-locking deadbolts or deadbolts that project at least 1 inch into the door frame or tumbler-type padlocks shall be used to safeguard unclassified and nonsensitive NASA supplies and equipment, if a lock is required.

(1) Selection shall be based on the value of items protected, mission essentiality, and vulnerability to threats.

(2) All questions regarding approved locks and locking devices shall be addressed to the individual Center Security Office and locksmith.

c. Padlocks and keys not in use shall be secured in a locked container that does not contain or store classified material, or in a locked room. Access to the container or room shall be controlled.

5.5 Key And Lock Accountability

a. Keys and combinations to locks shall be accounted for at all times. Individually issued keys to offices shall not be duplicated nor loaned out.

b. High security padlocks and their keys shall be inventoried by serial number semiannually. A written record of the inventory shall be retained, until the next inventory is conducted.

c. When a key to a high security padlock is lost or missing, an inquiry shall be conducted and the padlock replaced or re-cored immediately, if the situation warrants replacement.

d. A key and lock inventory shall be maintained, which includes a list of all of the following:

(1) Keys.

(2) Locks.

(3) Key serial numbers.

(4) Lock serial numbers.

(5) Location of locks.

(6) The number of keys maintained for each lock. This list shall be maintained and secured in the locksmith shop.

e. In coordination with the locksmith, facility service managers (FSM) shall conduct yearly inventories of keys for their facility and provide a copy of the inventory results to the locksmith. Discrepancies shall be rectified with the locksmith.

f. Rekeying and recoring of individual facilities shall be conducted when:

(1) Control and accountability of keys has been compromised.

(2) Requests for replacement of lost keys is equal to or greater than 25% of total issued keys for that facility or door in the facility. The organization responsible for the facility shall fund the rekey/recore activity.

(3) The facility is vacated and issued keys have not been recovered. The new occupant shall fund the rekey and recore activity.

g. High-security padlocks and keys that do not have a serial number shall be assigned one. This

number shall be inscribed on the lock or key as appropriate.

5.6 Additional Key and Lock Controls for Key Containers

a. Keys to key containers shall not be removed from the installation except to provide for protected storage elsewhere.

(1) Keys to locks securing key containers shall be afforded physical protection equivalent to that provided by the key container itself.

(2) Keys to containers shall be maintained separately from other keys, and shall be accessible only to those individuals whose official duties require access to them.

b. At no time shall keys be in the custody of a person not authorized to have them.

c. Under no circumstances shall keys and locks or alternate keys or locks be placed in any security container that contains or stores classified material.

(1) When arms and ammunition are stored in the same areas, keys to those storage areas shall be maintained together, but separately from other keys that do not pertain to AA&E storage.

(2) The number of keys shall be held to the minimum essential. Keys shall not be left unattended or unsecured at any time.

(3) Keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, shall be kept separate from other IDS keys.

(4) Access shall be permitted only to authorized maintenance personnel.

(5) IDS keys shall be stored in containers of at least 20-gauge steel equipped with GSA-approved low security padlocks or GSA-approved built-in three-position changeable combination locks, or in GSA-approved Class 5 or Class 6 containers that do not contain or store classified material. Combinations shall be recorded on SF 700 (Security Container Information), sealed in the envelope provided, and stored in a separate container.

(6) Security containers weighing less than 500 pounds shall be fastened to the structure with bolts or chains equipped with secondary padlocks to preclude easy removal.

d. In the event of lost, misplaced, or stolen keys, an administrative investigation shall be conducted immediately.

(1) The affected locks or cores to locks shall be replaced when practicable.

(2) Replacement or reserve locks, cores, and keys shall be secured to preclude access by unauthorized individuals.

e. Combination to locks on vault doors or GSA-approved Class 5 or Class 6 security containers shall be changed upon change of custodian, or other person having knowledge of the combination, or when the combination has been subject to possible compromise.

(1) Combinations shall also be changed when a container is first put into service.

(2) The combination shall be recorded using SF 700, sealed in the envelope provided, and stored in a container meeting local storage requirements.

(3) No other written record of the combination shall be kept.

(4) Controls shall be established to ensure that the envelopes containing combinations to locks are not made available to unauthorized personnel.

f. Replacement of lock cylinders and broken keys for high-security locks shall be coordinated with the local security office locksmith.

5.7 Additional Key and Lock Requirements

Aircraft and vehicle storage facilities in which vehicles or aircraft are permanently based with sensitive items onboard shall be outfitted, as appropriate, with security doors and frames (i.e., steel frames, metal-clad solid core doors), and secured with approved secondary high-security hasps and padlocks. Existing hangar doors are considered sufficient if properly employed at the end of each workday.

5.8 Chains

When a chain is required for security of unclassified but sensitive equipment and supplies, specifications for approved chains shall be obtained from the local security office.

5.9 Use and Control of Protective Seals

a. Purpose of the seal. The purpose of the seal is to show whether the integrity of a storage facility, vehicle, rail shipment, or container has been compromised.

b. A plain seal is not a lock, although combination items referred to as "seal-locks" are available.

c. The purpose of a seal, no matter how well constructed, is defeated if strict accountability and disciplined application are not maintained.

d. Ordering and storing seals. Seal construction specification shall include--

(1) Durability. Seals must be strong enough to prevent accidental breakage during normal use.

(2) Design. Seals must be sufficiently complex to make unauthorized manufacture of a replacement seal difficult.

(3) Tamperproof. Seals must readily provide visible evidence of tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.

(4) Individually identifiable. Seals must have embossed serial numbers and owner identification.

(5) Ordering and issuing. A single office on an installation shall be responsible for ordering and issuing seals. The source for the seals shall be instructed to ship the seals to the attention of a seal custodian in that office.

(6) Unused seals. Seals not issued for actual use shall always be secured in a locked, metal container with controlled access. Only seal custodians and alternates shall have access. Recorded monthly inventories shall be conducted to preclude undetected loss of seals.

e. Accounting for seals. Seal custodians shall maintain an IT-based seal logbook.

(1) The issuance process of seals to a using office, unit, or activity custodian shall reflect date of issue, name of recipient, and seal serial numbers.

(2) The issuance process of a seal for actual use by a custodian shall reflect the seal number, date and time applied, identification of items to which applied (and location on item if other than main door(s)), and the name of the person applying the seal. For outbound loaded trailers, railcars, and container shipments, the appropriate trailer, railcar, or container number and load destination shall be noted.

f. Application of seals.

(1) Seal all doors and openings, not merely the main one.

(2) Run seal straps through hasp only once. Seals wrapped around several times become illegible.

(3) Listen for "click" when inserting point of seal into sheath.

(4) To ensure positive closure, tug down on strap, and twist the point section inserted into the locking mechanism.

g. Checking seals. Centers using seals shall develop procedures for checking them. These procedures shall include actions to be taken to break a seal, and actions to be taken upon finding a broken seal.

5.10 Disposition of Used Seals

a. All shipping documents shall reflect seal number(s). All seals shall be verified with seal log, shipping documents, or other appropriate documents before removal and disposal.

b. Seals must be defaced sufficiently upon removal, so that they cannot be used to simulate a good seal. They shall be disposed of in normal trash.

c. If the user seal log is located on the same installation, the custodian shall be advised of the destruction of the seal, or the seal shall be returned to the custodian.

d. The custodian shall annotate the date and time removed, and the name of the individual removing the seal across from the original entry on the seal log.

5.11 Changing Seals

If used, the colors of seals shall be changed periodically, as an additional physical security measure.

CHAPTER 6: Protective Barriers

6.1 Purpose

6.1.1. To establish minimum criteria for physical security barriers and openings at NASA Centers.

6.1.2. Additionally, facilities and operations, when established under the provisions of the NASA mission essential infrastructure protection program (MEIPP), must meet specific criteria established in Chapter 6 of this NPR.

6.1.3. Physical barrier requirements are designed to deny, impede, or discourage access to NASA areas by unauthorized personnel or groups. This is accomplished by one or more of the following:

6.1.3.1. Defining the perimeter of the installation and any security areas.

6.1.3.2. Creating a physical and psychological deterrent to entry, as well as making a legal statement that entry is not permitted.

6.1.3.3. Delaying intrusion into security areas, thus making more likely the detection and apprehension of intruders by protective forces.

6.1.3.4. Facilitating the effective and economical utilization of protective forces.

6.1.3.5. Directing the flow of personnel and vehicles through designated portals, in a manner that permits efficient operation of a personnel identification and control system.

6.2 Types of Barriers

6.2.1. Protective barriers are divided into two major categories: natural and structural.

6.2.1.1. Structural barriers are manmade devices such as fences, walls, floors, roofs, grilles, bars, roadblocks, or other structures that deter penetration.

6.2.1.2. Natural barriers may be forests, rivers, swamps, beaches, or other terrain difficult to traverse.

6.3 General Considerations

6.3.1. Established physical security barriers at NASA Centers are not designed to stop a determined intruder, but rather to deter or delay.

6.3.2. Such barriers, depending on area security, should be augmented by security personnel and IT-based surveillance and monitoring systems, when warranted.

6.3.3. When planning or establishing security barriers at NASA Centers, the CCS shall consider the following, prior to recommending security barriers:

6.3.3.1. Physical barriers that are as personnel-proof as economically feasible should be established around all security areas. The type of barrier used should be determined after a study of local conditions has been made by the CCS and facilities engineering professionals with security engineering backgrounds.

6.3.3.2. In some instances, the temporary nature of the security interest makes the construction of costly permanent physical barriers impracticable and unjustifiable. In such cases, the security interest must be protected by other means, such as use of temporary barriers, additional protective forces, patrols, and other compensating protective measures.

6.3.3.3. In cases of extreme criticality and vulnerability of NASA facilities, it may be necessary to establish two lines of physical barriers at the security area to be protected.

6.3.3.4. The immediate boundaries of a NASA Center and any specific designated security area shall be fenced. As a minimum, "U.S. Government-No Trespassing" signs with appropriate prosecution warnings shall be attached not more than 100 feet apart along, and at each corner of, the boundaries of the land. This defines the perimeter, provides a buffer zone, facilitates control, and makes accidental intrusion unlikely.

6.3.3.5. In establishing any perimeter barrier at a NASA Center, due consideration must be given to providing emergency entrances and exits in case of fire.

6.3.3.6. The size of an individual internal security area shall depend on the degree of sensitivity required and the complexity of the area. As a rule, size should be kept to a minimum consistent with operational efficiency. Positive barriers at NASA Centers shall be established for:

a. Controlling vehicular and pedestrian traffic flow.

b. Checking identification of personnel entering or departing.

c. Conducting random vehicle checks.

d. Defining a buffer zone for more highly classified or sensitive areas.

6.3.4. Individual Center geographical and environmental characteristics, specifically water and marshland boundaries, present special security problems. Such areas at any Center should be defined by appropriate fencing and signs.

6.3.5. Construction of new security barriers and removal of existing barriers and related work must be approved by Center Security, and scheduled to provide a continuous level of security for the activity/program.

6.4 Temporary Barriers

6.4.1. In some instances, the temporary nature or infrequent existence of a sensitive program/project requiring security constraints does not justify the construction of more permanent physical perimeter barriers.

6.4.2. In such cases, a Center-designated limited area or closed area of temporary nature and short duration may be established, in which the reduction of security resulting from deficiencies in physical barriers is compensated for by additional security forces, patrols, and other security measures, during the period of restriction.

6.4.3. Barricade requirements include jersey barriers, blast resistant concrete wall construction, and

security fencing.

6.4.4. In any case, a designated temporary security area shall not exceed 30 days from date of installment without specific authorization from the CCS.

6.4.5. The use of wire barriers or similar construction for temporary enclosures is recommended as being both expeditious and effective, with a minimum use of security forces required to control and safeguard the area.

6.5 Security Fences

6.5.1. Security fences at NASA Centers should enclose all designated security areas, and shall be constructed in such a manner that they are reasonably impassable.

6.5.2. The nature of the security area shall determine the degree of restriction of movement of personnel, vehicles, and equipment necessary for adequate security.

6.5.3. The Center CCS must approve all security fence requirements and, prior to approval, shall assess the permanency of the security area, availability of materials, presence of natural aids to security, Center security personnel, security vulnerabilities, and the degree of security required.

6.6 Security Fence Standards

6.6.1. Chain-link fencing shall be the type of structural barrier most commonly used and recommended for security purposes at NASA Centers, and should enclose all designated security areas.

6.6.2. The following fence standards shall apply.

6.6.2.1. Fabric. The standard fence fabric shall be at least 9-gauge zinc- or aluminum-coated steel-wire-chain link with mesh openings not larger than 2 inches per side and a twisted and barbed selvage at top and bottom.

6.6.2.2. Fabric ties. Only 9-gauge-steel ties with coating compatible with the fabric shall be used. In lieu of wire ties on fence posts, approved fabric clamps can be used. In lieu of wire ties on bottom and top taut wires, hog clamps may be used. Spacing between ties should not exceed 12 inches.

6.6.2.3. Height. The preferred height of any NASA security fence is 9 feet. This includes, at a minimum, a fabric height of 8 feet, plus a 1-foot barbed-wire top-guard. Concertina (Razor) wire may be used in lieu of the barbed-wire top-guard to provide added protection against intrusion for areas of high sensitivity. Building connections shall be higher. Fencing 12 feet high from the connection point of the building to the distance of 12 feet from the building is recommended, unless the building wall itself is less in height.

6.6.2.4. Fencing posts, supports, and hardware. All posts, supports, and hardware for security fencing shall meet the requirements of Federal Specification RR-F-191K/GEN of May 14, 1992, unless superceded by later issuance. All fastening and hinge hardware shall be secured in place by peening or spot welding to allow proper operation of components, but prevent disassembly of fencing or removal of gates. All posts and structural supports shall be located on the inner side of the fencing. Posts shall be positively secured into the soil to prevent shifting, sagging, or collapse. Fence posts should be placed no more than 10 feet apart and mounted in concrete 36 inches deep. The diameter of the concrete shall not be less than 10 inches for line posts, and not less than 12 inches for corner and gate posts.

6.6.2.5. Reinforcement. Taut reinforcing wires (at least 9 gauge) shall be woven through, or affixed with, the fabric along the top and bottom of the fence for stabilization of the fence fabric. Top and center rails should not be used, as they may provide added assistance for climbing.

6.6.2.6. Ground clearance. The bottom of the fence fabric must be within 2 inches of firm soil, or buried sufficiently (concrete footings or gravel may be used) in soft soil to compensate for shifting soil.

6.6.2.7. Culverts and openings. Culverts under or through a fence shall be of 10-inch pipe or of clusters of such pipe or its equivalent. Openings under or through a fence shall be secured with material equal or greater in strength than the overall barrier.

6.6.2.8. Fence placement. No fence should be located so that the features of the land (its topography) or structures (buildings, utility tunnels, light and telephone poles, fire escapes, ladders, etc.) defeat its purpose by allowing passage over, around, or under the fence.

6.6.2.9. Topguards. Topguards are constructed on perimeter fences and may be added on interior enclosures for additional protection. A topguard is an overhang of barbed wire along the top of a fence, facing upward and outward, at approximately a 45-degree angle. Topguard supporting arms shall be permanently affixed to the top of fence posts to increase the overall height of the fence by at least 1 foot. Three strands of 12-gauge barbed wire, spaced no more than 6 inches apart, must be installed on the supporting arms. The topguard of fencing adjoining gates may range from a vertical height of 18 inches to the normal 45-degree outward protection, but only for sufficient distance along the fence to open the gates adequately.

6.7 Barriers

6.7.1. Buildings, structures, waterfronts, and other barriers used instead of (or as a part of) a fence line should provide equivalent protection to the fencing required for that area.

6.7.2. All windows, doors, and other openings must be provided adequate protection (e.g., wire mesh caging), or properly secured.

6.7.3. Walls

6.7.3.1. Where walls, floors, or roofs serve as barriers, they should be constructed and arranged to provide uniform protection equivalent to that provided by chain-link fencing as specified.

6.7.3.2. In this connection, windows and other openings in perimeters of security areas in any of the following categories should be protected by securely fastened bars, grills, or other equivalent structural means.

a. Openings less than 18 feet above uncontrolled ground, roofs, ledges, etc.

b. Openings less than 14 feet directly or diagonally opposite uncontrolled windows in other walls, fire escapes, roofs, etc.

c. Openings less than 6 feet from uncontrolled openings in the same wall.

6.7.4. Perimeter Openings

6.7.4.1. Openings in perimeter barriers shall be kept to the minimum necessary for the safe and efficient operation of the Center.

6.7.4.2. The CCS, in coordination with facilities engineering, safety and fire, shall approve all

openings.

6.7.4.3. Authorized barriers shall be constantly locked, controlled by authorized personnel, or otherwise secured to prevent unauthorized entry or exit.

6.7.4.4. Those areas that cannot be secured because of safety/fire hazards may be secured utilizing lead seals.

6.7.4.5. When locked and not under constant surveillance, they shall be subject to periodic checks by protective forces or other designated personnel and/or monitored by security surveillance cameras.

6.7.5. Gates.

6.7.5.1. Gates are designed to facilitate the entrance and exit of authorized personnel and vehicle traffic, and to control its flow.

6.7.5.2. The CCS, in coordination with facilities engineering, safety and fire, shall establish gate operations and designations.

a. Designated gates shall be limited to the number consistent with efficient operations and traffic flow.

b. Alternative gates, which are closed except during peak movement hours, may be provided, so that heavy traffic flow can be expedited.

c. When open or operating, all gates shall be under continuous positive control.

d. Gates shall provide protection equivalent to the outer fences or barriers of which they are a part when not in use. These gates shall be locked to form an integral part of the established perimeter when secured.

6.7.6. Pedestrian gates.

a. Approved pedestrian gates and turnstiles shall be channeled in such a manner that allows only one person entering or departing to approach the custodial sentry at a time.

b. Some channels may be closed between peak use hours.

c. Where possible, pedestrian and vehicular gates should be clearly separated.

d. All vehicle gates shall be equipped with a center stabilizing rod and hole.

6.7.7. Vehicle Gates.

6.7.7.1. Where feasible, approved vehicle gates should be set well back from any public highway, so that temporary delays caused by identification control checks at the gate shall not cause traffic hazards extending out onto a public highway.

6.7.7.2. There should also be sufficient space at the gate to allow for spot checks, inspections, searches, and temporary parking of vehicles, without impeding the flow of traffic.

6.7.8. Inspection

6.7.8.1. When gates are not in active use, they shall be locked and frequently inspected by security personnel.

6.7.8.2. Locks shall be serviced as required. The CCS shall assure security and accountability for the keys to locks on these gates per Chapter 5 of this NPR.

6.8 Doors, Windows, and Skylights

6.8.1. Building or egress doors at NASA Centers or at the secure area perimeter should provide the protection (e.g., metal doors, secure hinges, fastened pins, or inside heavy-duty hasps and staple set) commensurate with the requirement for proper protection of the assets accessible through those doors.

6.8.2. Windows, skylights, and other openings that penetrate the perimeter barrier and have a security mesh or grating area of 96 square inches or greater should be protected in such a manner as to preclude physically breaching the opening.

6.8.3. Use of protective screens is recommended when the threat level is such that the screens could provide the additional value of preventing missiles, such as hand grenades, bombs, and incendiaries, from being hurled through the windows from outside the perimeter.

6.9 Sewers, Culverts, and Other Utility Openings

6.9.1. Sewers, air intakes, exhaust tunnels, and other utility openings that penetrate the perimeter or security area barrier and have a cross-section area of 96 square inches or greater shall be protected by securely fastened bars, grilles, locked manhole covers, or other equivalent means that provide security commensurate to that of the perimeter or security area barrier.

6.9.1.1. As a reminder, these bars and grilles across culverts, sewers, storm sewers, etc. are a hazard when susceptible to clogging, and should be considered during planned construction of such bars and grilles.

6.9.1.2. All such areas should be designed to permit rapid clearing or removal of grating when conditions require such action.

6.9.1.3. Removable grates shall normally be locked in place.

6.10 Utility Poles and Trees

Poles and trees located outside or inside of and within 10 feet of the perimeter barrier of the security area present a possible means of illegal entry. To reduce this possibility, the perimeter barrier may be adjusted so as to increase the distance to more than 10 feet and heightened to the extent necessary to prevent entry, or the obstruction must be removed. If these utility poles, signboards, trees, etc. also obstruct the visibility of the security officer, they must be moved (or removed) at least 10 feet outside or inside the perimeter barrier.

6.11 Clear Zones

6.11.1. Designated security areas and protective barriers at NASA Centers shall maintain unobstructed areas or clear zones.

6.11.2. The unobstructed areas or clear zones should be maintained on both sides of and between physical barriers.

6.11.3. This shall be accomplished by removal of all trees, brush, rock piles, etc. within the designated zone and the frequent cutting of vegetation or the use of chemicals designed to control or

kill such vegetation.

6.11.3.1. Vegetation shall not exceed 8 inches in height.

6.11.4. These areas shall be kept free of vehicles, structures, and debris.

6.11.5. Protective barriers inside a clear zone should be at least 10 feet from the perimeter.

6.11.6. Where possible and when the sensitivity of the activity requires a larger clear zone, it should be provided to preclude/minimize damage from thrown objects such as incendiaries or bombs.

6.11.7. Protective barriers outside clear zones shall be 10 feet or more from the perimeter fence/protective barrier and any exterior structures, vegetation, or any obstruction to visibility.

6.11.8. Construction of any new protective barrier for security operations having a smaller clear zone must be coordinated with facilities engineering, safety and fire, and approved by the CCS.

6.11.9. Although 10 feet is the permissible minimum criteria for NASA Centers, every effort shall be made to establish a clear zone external to the protective barrier of 75 feet.

6.11.10. The minimum NASA standard clear zone for effective surveillance of the perimeter terrain when planning new activities or expansion of existing activities is 10 feet inside the barrier, 10 feet between barriers/fences, and 10 feet exterior to the boundary fence.

6.11.11. In addition to security, these clear zones also provide the safety feature of a 60-foot-wide fire-break between a Center's operational areas, structures, or storage facilities and the adjoining areas. It is especially important to maintain clear zones during periods of high fire risk.

6.12 Inspection and Repair of Barriers

6.12.1. Center security or other designated personnel shall periodically check designated barriers for defects that would facilitate unauthorized entry. Both Center security and other personnel must be alert to detect the following:

6.12.1.1. Damaged areas (cuts in fabric, broken barbed wire/ posts).

6.12.1.2. Deterioration (corrosion).

6.12.1.3. Erosion of soil beneath the barrier.

6.12.1.4. Loose-fitting barbed wire, outriggers, or fabric fastener.

6.12.1.5. Growth in the clear zones that would afford cover for possible intruders.

6.12.1.6. Obstructions at or on the fence that would afford concealment or aid entry/exit for an intruder.

6.12.1.7. Evidence of illegal or improper entry.

6.12.1.8. Damaged or tampered lead seals in place.

6.13 Signs and Posting of Boundaries

6.13.1. The boundaries of NASA Centers shall be posted with signs having the wording "RESTRICTED AREA - NO TRESPASSING" (NASA Form 1506) in 2-inch red/black letters. (See Appendix G for other signs.)

6.13.2. Signs shall be located on the exterior side of the Center perimeter barrier or mounted on posts along the boundary line.

6.13.3. The interval between signs shall be adequate to permit at least one sign visible and legible during daylight hours to anyone approaching the boundary from outside the Center.

6.13.4. All designated security areas or spaces shall be plainly identified by signs reading "RESTRICTED AREA," "LIMITED AREA," or "CLOSED AREA."

6.13.4.1. These signs shall further bear in small lettering the words, "Unauthorized Persons Who Enter May Be Subject to Prosecution Under 18 U.S.C. 799."

6.13.4.2. Signs shall be placed on the outward edge of the clear zone or security areas and on the perimeter fence.

6.13.4.3. The purpose of this placement is to prevent unintentional approach to the security area barrier through the clear zone.

6.13.4.4. Signs shall be spaced such that they are visible and legible to anyone approaching the security area from any direction.

6.13.5. All roads approaching the security area shall be clearly posted with restrictive-entry signs.

6.13.6. The requirements contained herein are considered the minimum acceptable.